A Work Project, presented as part of the requirements for the Award of a Master Degree in Management from the NOVA – School of Business and Economics.

THE IMPLICATIONS OF GDPR FOR SOFTINSA – Advanced Software Engineering, Lda.

MIGUEL FILIPE AMARAL PORTAS, 3670

A Project carried out on the Master in Management Program, under the supervision of:

Professor Leonor Rossi

June 5th 2018

INDEX

ABSTRACT

The aim of this Work Project, carried out under the method of Direct Research Internship, is to provide a clear overview of the potential implications of the General Data Protection Regulation (GDPR) to the Global Business Services company *Softinsa – Advanced Software Engineering, Lda*. The enforcement of the GDPR will impose new costs due to the need of implementing Technical and Organisational Measures (TOMs). It will also force changes from a structural perspective, such as hiring additional legal experts. Finally, the GDPR will impose significant restrictions regarding the processing of personal data, carried out by *Softinsa*.

1. INTRODUCTION

1.1. Objectives of the Internship

The writing of this Work Project went hand in hand with a Curricular Internship the student has carried out, for five months, at *Softinsa – Advanced Software Engineering, Lda*., an *International Business Machines (IBM)* Group undertaking. The student was integrated into the Global Business Services sector, specifically on the field of SAP, a software used to plan a company's resources, globally, and to manage data programs. This SAP field is mainly dedicated to the implementation and maintenance of SAP systems, which encompass diverse information concerning personal data, including companies' stakeholders' details, namely employees', clients' and suppliers' personal data. The concept of personal data is fundamental to interpret the GDPR guidelines. In turn, the GDPR refers to personal data as any sort of information which, either directly or indirectly, leads to the identification **of a human being** (as opposed to the identification of an artificial legal person, such as a corporation), as will be clarified below in Section 2, deeply.

Actually, managing the access to personal information, whether purposefully or incidentally, is the core issue covered by the General Data Protection Regulation (GDPR) guidelines that are, in turn, the bulk of this dissertation.

WHY A WORK PROJECT ON GDPR?

The objectives of this Internship consisted in: firstly, assessing and validating the new processes carried out in order to ensure compliance with the GDPR, with regard to the Clients to whom the company provides its services, as a Processor; secondly, performing a critical analysis of the impact of GDPR, from a financial (additional costs), behavioural and structural perspective, on *Softinsa*.

Thus, the main focus of this Report will lie on providing the readers a clear overview of the potential implications of the GDPR for the Global Business Services company *Softinsa*.

1.2. Softinsa

Softinsa – Advanced Software Engineering, Lda. is an *IBM* and *Viewnext* Group company, which operates in the Global Business Services industry. In fact, 49% of the undertaking is held by *IBM Portugal* and the remaining 51% are detained by the Spanish corporation *Viewnext*, which by its turn is an *IBM Spain* subsidiary (as shown on the pie chart below). The firm specialises its business activities in a wide portfolio of services such as Application Management Services, Analytics, Human Capital Solutions, SAP Consulting and Maintenance Services and IT Managed Services.[i] As a traditional B2B (Business-to-business) undertaking, its main **clients** are other undertakings from diversified sectors: *Galp Energy* and *PRIO Energias* from the Energy & Utilities industry; *Novo Banco* and *Caixa Geral de Depósitos* from the Banking sector; *Portugália* and *Pestana Group* from Catering and Hotel markets respectively; *Centro Hospitalar Lisboa Norte* (commonly known as *Hospital de Santa Maria*) concerning the Healthcare sector.

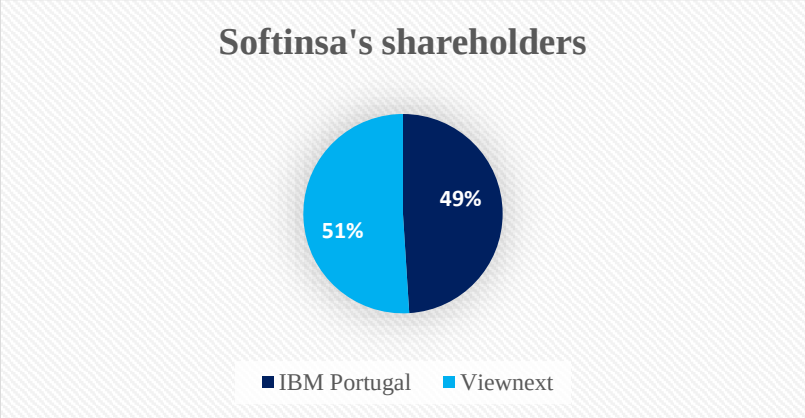

Figure 1 – Distribution of the company's shares between *IBM Portugal* and *Viewnext*

1.3. The access to personal data by *Softinsa*

In order to provide its SAP Maintenance and Management services, *Softinsa* might have, **and here the perspective that most interests us**, access to personal data concerning its clients' third parties (what includes **staff** and **suppliers**), through the software. Under the new Regulation, the GDPR, this context transforms *Softinsa* into a data processor, since the company is processing personal data on the behalf of the Client as it will be explained further on this Work Project (section 3.2.).

In addition, *Softinsa*'s Human Resources department has access, as expected, to data related to **staff**, controlling the employees' registration. Furthermore, the Purchasing Department accesses the personal data from suppliers, including their banking and tax details.

Throughout the Internship, it was observed that a *Softinsa*'s SAP Consultant using SAP to perform his/her tasks, could have access to or be exposed to sets of information including *inter alia* personal data collected about third parties, but by the client. On the one hand, this happens, for example, when dealing with the client *Lisnave*, a Portuguese nautical transport construction and repair undertaking. Conversely, this occurrence is not verified for example within the Healthcare sector (e.g. since the SAP Consultant logs on the software to serve the client *Hospital de Santa Maria*, the access to employees' and patients' personal data are not available in SAP).

1.4. The enforcement of a new legal framework

On May 25th 2018, a new European Union Regulation[II] – a binding legislative act that applies in its entirety to all European Union's Member-States, to its residents, citizens, public entities and private corporations – will come into force, in order to provide a higher level of protection of personal data, within the European Union. The new General Data Protection

Regulation will be implemented simultaneously in the 28 Member-States of European Union, on the mentioned data, and will replace the former 1995 Directive[1] concerning data protection.

The application of the new Regulation will imply changes in the manner personal data is processed by *Softinsa* and consequently in its interaction with Clients, bring about additional costs to ensure compliance, lead to a structural change within *Softinsa* and impose many restrictions regarding the access to natural persons' personal data.

2. THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

The rapid technological progress and globalisation the world has been facing over the last couple of decades, has led to an expansion of the share and collection of information worldwide. That is, individuals have been increasingly making personal information available, willingly, publicly and globally, mainly through the use of networks from a social and professional nature.

On one hand, technology enables both private undertakings and public authorities to make use of personal data in order to carry out their activities, whilst ensuring a high level of protection of those data.

On the other hand, a dark consequence of Information Technology must not be ignored. The fast and outstandingly powerful digital transformation has permitted the evolution of new and sophisticated hacking techniques, augmenting the risk of personal data breach, theft and loss, exposing individuals to a higher likelihood of being identified (and tracked) and thus violating natural persons' fundamental rights.

[1] Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31)

Therefore, due to these developments, the enforcement of a new legislation bringing a stronger data protection framework to the European Union is justified.

2.1. The aim, purpose and addressees of the Regulation

The primary purpose of the European Union General Data Protection Regulation, GDPR, is twofold: to protect the fundamental rights and freedoms of natural persons regarding the processing of their personal data, and to facilitate the free flow of personal data, within the European Union.

From the point of view of the **subjects** involved, the Regulation is applied to: (a) every single natural person, public institutions or private undertakings within the Union processing European Union's citizens' personal data and to (b) any individual, private and public entities and organisations **even outside the European Union** that perform the processing of personal data that concerns to natural persons from the European Union.

The main challenge in understanding the GDPR is that it spells out a set of key **concepts and roles**, namely on its Article 4[III]. In order to provide a clear and appealing overview of those to the reader, only 8 will be listed:

a) ***Natural person*** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

b) ***Personal data*** refers to any information concerning an identified or identifiable natural person; within personal data there is a distinction between direct identifiers – to be used to identify a natural person without additional information – and indirect identifiers – does not identify an individual by its own but it so if combined with additional data points from other sources (e.g. birthday and location)

c) ***Personal data breach*** includes any violation of security with the ultimate consequence of an unintentional or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed

d) ***Processing*** encompasses any operation or set of operations which is(are) performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

e) ***Data controller*** is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data

f) ***Data processor*** is a natural or legal person, public authority, agency or other body which carries out the processing of personal data on behalf of the Controller

g) ***Data Protection Officer*** *(DPO)* is a person within the undertaking to whom the duty of ensuring the organisation's awareness regarding GDPR and compliance with the legislation is entrusted

h) ***Supervisory Authority*** is an independent public authority which is established by a Member – State to be accountable for the application of the Regulation on that nation and for providing guidance on its comprehension.

2.2. The content of the GDPR

In order to attempt to explain what the subsequent articles of the Regulation actually mean, the structure of the Regulation begins with 173 recitals[2]. Moreover, the GDPR's structure and comprehension are complex, since they imply a tremendous effort in reading the recitals in conjunction with the articles they concern.

After the analysis of the introductory 173 recitals of the GDPR, it is possible to interpret its content, applying it to *Softinsa*. Thus, under the terms of the Regulation under discussion[IV]:

(1) The Controller (role played by the Client) determines the purposes and ends for the processing and the Processor (*Softinsa*) is accountable for the processing activity on behalf of the Controller;

(2) Both data Controller and Processor are liable for breaches of confidentiality concerning natural persons' personal data;

(3) The processing of personal data for any non-professional or rather non-commercial purpose is not included;

(4) The Regulation provides for situations in which competent authorities are allowed to process and use personal data for protection, investigation, detection or prosecution of criminal offences and directors' and officers' liability or execution of criminal penalties;

(5) Wherever the processing of data is carried out by a group of undertakings, the processor's main establishment is the group's, unless the means and the ends of processing are determined by a third corporation;

[2] "From the European Law perspective, a recital is a text that explains the reasons leading to a legislative act, without the use of normative language neither political argumentation. By convention a recital begins by the expression *Whereas*".

(6) The processing of personal data is lawful, where it does not deviate from the purpose it has been processed for, regardless that end was to serve public interest, scientific, historical or genealogical research or merely statistical purposes;

(7) The general principles of data transfer between a group of undertakings and a third entity remain unchanged;

(8) the transfer of personal data between undertakings in which one of them is outside the EU/EEA (European Economic Area) is lawful, since the appropriate safeguards for the transfer are guaranteed;

(9) It is mandatory that each Member – State from the European Union establishes a Supervisory Authority to verify the enforcement of the Regulation's requirements. Each Member – State retains the freedom circa which entity, within the national boundaries, will be entrusted with the task;

(10) Fines or rather merely reprimands may be imposed to offenders, taking into account the nature, the seriousness and the duration of the infringement, the degree of responsibility or any other previous infractions recorded;

Finally **(11)** the Regulation sets out a clearly defined set of rights the data subjects involved retain, concerning the processing activity.

3. POTENTIAL IMPLICATIONS OF GDPR FOR *SOFTINSA*

3.1. The Responsibilities and duties of *Softinsa* as a Controller

The main duty of a Controller is to determine the means and the purposes for the processing of personal data and to ensure that processing activities are performed under the consent of data subject(s).

Although on the majority of occasions *Softinsa* plays the role of Processor, by just carrying out the processing activity on behalf of the Client, the company may also behave as a Controller.

Take, for example, situations in which the company processes its staff's personal data[3], for posterior consultation by the Human Resources department as mentioned in the Introduction section. In these cases, *Softinsa* is acting as a Controller, within the framework of the GDPR, and needs to fulfil a set of responsibilities.

The first one lies on keeping the basic principles of processing of natural persons' personal data stated by the Regulation such as ***transparency*** to the data subject, ***lawfulness***, ***purpose limitation***, ***accuracy***, ***integrity*** and ***confidentiality***.

Moreover, it is up to the Controller to implement technical and organisational measures (TOMs) that mitigate the risk of data breach and to demonstrate the processing activity is aligned with the requirements of GDPR[V].

Wherever the means and the purposes are determined by more than one Controller, *Joint* Controllers, an agreement that clarifies the responsibilities to be taken by each Controller concerning the compliance with the GDPR guidelines, in particular as regards the exercising of the rights of the data subject as well as their roles and relationships in relation to the data subject, must be sealed under total transparency[VI].

The duty of notifying the Supervisory Authority of any breach, within 72 hours after the acknowledgement of the transgression, must be taken into account by Controllers. The notification should provide, whenever possible, the nature of the data breach, the categories of data and the number of subjects affected, the identity and contact details of the Data Protection

[3] Actually, whenever Softinsa is processing its staff personal data it is acting **as a Controller as well as a Processor.**

Officer in charge and a brief description of the potential consequences resulting from the violation.

At last, Controllers are also required by GDPR guidelines to inform the data subject on the rights they are provided concerning the processing activity (referred on section 3.3). Nevertheless, the Controller is fully exempt of this duty wherever it cannot identify the data subject.

3.2. The Responsibilities and duties of *Softinsa* as a Processor

The new European Union data protection legislation, the GDPR, will have an impact on the agents processing personal data of natural persons linked to the EU[4]. Processors are the party involved that will feel those changes more significantly, since the new law will bring them specific obligations they were exempt until its enforcement.

By definition, a Processor is the one processing personal data on behalf of the Controller. This means that, as a Processor, *Softinsa* is required to follow the Controller's instructions (the role of Controller is here assumed by the Client) and so is also subject to the responsibilities imposed to Controllers. In fact, the Processor is appointed by the Controller with the requirement that the first party demonstrates ability to come up with suggestions regarding technical and organisational practices (the decision on its implementation is, as explained before, up to the Controller) that mitigate the risk of natural persons' exposure to the risk of data breach, theft or loss.

[4] In the past, these issues were regulated by a Directive: Directive 95/46/EC of the European Parliament and of the Council of the 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31)

Processors may also contract sub processors to perform the treatment of personal data, on which the Regulation poses no hurdles. However, this scenario requires that Controller, whoever retains the right to object, gives its prior consent.

Furthermore, *Softinsa*'s processing activity, as a Processor, is required to be regulated by a binding contract jointly with the Controller, the *Data Processing Agreement* (DPA). The agreement must cover the duties the Processor is subject to like the duration, nature and purpose of the processing and the categories of personal data that will be processed and the rights and obligations of the Client. Moreover, it is a duty of the company to inform the Client immediately of any instruction or procedure that may end up at GDPR violation, such that the Processor is exempt of any liability for infractions practiced.

The main challenge Processors will face consists on ensuring compliance with the terms of this legislation. Such task will require to keep a record of all processing activities – including details of the agents involved, Data Protection Officer's information, transfers of data to third countries[5] and a description of the Technical and Organisational Measures implemented – that may be requested by the Supervisory Authority that will monitor compliance in Portugal[VII].

3.3. The rights of the data subject(s)

Within the framework of the GDPR, a data subject differs from a Controller at the extent that the first refers to a natural person, whose personal data was processed to serve a specific purpose, set by the Controller.

The General Data Protection Regulation anticipates a set of rights that data subjects retain, regarding the processing of their own personal details. It is intuitive that part of those rights will complement or even overlap the main duties of the parties involved in the processing activity, that is Controllers and Processors[VIII]:

[5] In the terms of an European Regulation, a third country refers to a nation or State located outside the European Economic Area.

The right of Transparency:

Transparency in communication between the Controller and the data subject is essential to demonstrate that processing is carried out under a lawful and fair procedure. Thus, a minimum of information, including mainly the identity of the Controller and the reasons for processing, is required to be provided by the Controller to the data subject, in order to address the transparency principle;

The right to access:

In addition, **the right to access to their own personal data** must not be denied to subjects. Data subjects have the right, to access their personal data in order to confirm if Controllers are processing their data and be informed on the purposes of processing and the categories of data processed, the timeframe of the processing activity and the rights to demand erasure, rectification, restriction and complain to the Supervisory Authority wherever a breach occurs. In case the data subject demands excessive or unjustified requests, the Controller has authority to charge fees in order to cover the administrative costs to attend the subject's request. Nevertheless, it is the Controller's responsibility to demonstrate the unfounded or excessive nature of such requests.

The right to rectification:

The data subject(s) retain(s) the right to rectification which requires that inaccurate, incomplete or incorrect data are deleted or properly rectified, by Controllers.

The right "to be forgotten" vs the right to restriction of processing

The data subject has the right to request the erasure of his/her personal data where the processing of those is not serving its purpose anymore, the processing is following an unlawful procedure or simply the data subject wishes to withdraw his/her consent and there is no longer

a lawful ground to continue the processing activity. This principle is also known as "the right to be forgotten". However, the GDPR also provides for circumstances under which data subjects are not allowed to request the erasure of data, since the Controller detains lawful basis for processing. Even so, the subject is entitled to restrict the purposes of processing (e.g. to exercise or the defence of legal rights, to protect another natural person or entity or even to serve a public interest cause). This is an affair still too vague within the framework of the GDPR.

The right to data portability:

The Regulation gives the natural persons who hold the personal data under processing the right to have no hurdles on the transfer of those data between Controllers, to receive a copy of their personal data in a structured, commonly used format that allows its reuse, and to the storage of their own personal data on a private device for posterior consultation.

The right to objection to processing:

Wherever the lawful basis for processing is related to public interest defence, direct marketing, statistical ends, historical or scientific research purposes or rather legitimate interests of the Controller, the GDPR gives the subject the right to object to the processing activity. Unless the Controller is able to invoke lawful grounds that overweigh the interests, rights or freedoms of the subject, it is required to cease the processing of personal data.

To conclude, this wide range of rights may lead to potential limitations for *Softinsa* and other undertakings concerning the processing of personal data, aligned to the guidelines of this new legislation, bring about more administrative costs for companies in order to address the bureaucracies involved and even alter the undertaking's business model[IX].

SERIOUS TRAITS OF GDPR FOR SOFTINSA

3.4. Criminal offences and Directors' liability

The enforcement of this new strict and tight Regulation concerning natural persons' personal data protection combined with the unstoppable technological progress, worldwide, has led to a higher top management liability with regard to cyber security issues, such as personal data breach or data misuse and any damage suffered by data subjects due to the breach.

It is relevant to clarify that companies' top management responsibilities for data protection legislation compliance is not that new, since the liability was already allocated to them, at some extent, even before the GDPR enforcement in May 2018. Either way, the risk of exposure not only to harmful penalties but also to potential reputational damages for the business will pressure directors and officers to adopt initiatives to address the increased risk of personal data violations. The request for personal data's encryption (converting personal data into an unreadable content for unauthorized users) could be a solution. However, it is expectable that there will be not many Clients willing to cover the underlying costs.

From an international perspective, the United Kingdom established on September 2017 a new legislative act that enforces senior managers' duties towards data protection. The new *Data Protection Bill* states, on its section 177[X], that organisations and their directors, managers, secretaries or similar officers will be considered guilty and liable for any infringement of data protection principles performed under those officers 'connivance, consent or associated to those executive officers' negligence. Additionally, other nations within the European Economic Area such as Italy and France have also followed the same steps of UK on this matter, enhancing the executive liability regarding failure at compliance. In order to mitigate the risk of breach of the Regulation, directors should adopt a superior risk management culture, what includes encouraging a sophisticated cyber and IT risk management[XI].

To conclude this topic, it is vital that senior management bear in mind that data processing must be performed under total transparency to data subjects and controllers, in order

to avoid any sort of penalties and administrative fines imposed on companies, that may represent quite heavy punishments, as we shall check next.

3.5. Fines and Penalties for Infringement

Non-compliance with the terms of the Regulation might lead to the imposition of heavy sanctions and penalties to companies, depending on the seriousness of the breach, on the implementation (or lack of) of preventive measures and actions taken in order to minimise the damage for data subjects and the record of previous transgressions.

Wherever a data subject wishes to report a violation of the terms of GDPR concerning his/her own personal data, that complaint should be directly reported to the national entities duly designated for that purpose and the respective compensation requested to the civil courts of the Member-State. With regard to Portugal, complaints reporting data breaches, any processing activity without the subject's consent or any other irregularity associated to non-compliance are directly reported to *Comissão Nacional de Proteção de Dados* (CNPD).

In case an organisation fails at properly filling and organising its records, notifying the Supervisory Authority and the data subject when a breach takes place and conducting appropriate risk analysis regarding data breaches, the lower level of fines may be invoked. That is, the undertaking may be charged a fine up to 2% of the prior financial year's turnover, worldwide, or rather €10 million, depending on whichever is the greatest amount.

Wherever the company violates the basic guidelines concerning personal data security or rather processes personal data by violating the data subject consent, the upper level of sanctions is applied and the offending undertaking is subject to a fine up to 4% of the prior financial year's turnover, worldwide, or rather €20 million, depending on whichever is the heaviest value. The purpose of the application of the sanctions above is to raise the directors' and officers' commitment to the implementation of cyber security measures aimed at addressing potential cyber-attacks that may end up at data breaches[XII].

3.6. The Importance of the role of the Data Protection Officer (DPO)

The enforcement of GDPR will lead to substantial alterations on the way organisations, subject to the new legislation, perform their business operations involving processing activities. The complexity and difficulty associated to compliance obligations, will bring about considerable costs for undertakings not only due to the need of implementing Technical and Organisational Measures to mitigate the risk of transgression but also due to the necessity of hiring new legal experts and nominating a Data Protection Officer (DPO). The DPO will be the person, within *Softinsa*, accountable for raising GDPR awareness and ensuring compliance with the new data protection legislation requirements. Therefore, the Data Protection Officer works as an advisor who informs Controllers and Processors about their obligations under the new law, supervises the compliance with GDPR by the Controller and Processor, ask the organisation for Impact Assessments and cooperate with the Supervisory Authorities in order to transmit transparency to the data subject(s)[XIII]. In order to perform his/her duties, the appointed officer must be given the power to investigate and void potential data breaches within the organisation.

Although the Regulation does not demand a specific professional profile for the nominated DPOs, it is recommendable that the officer is someone who owns an expert knowledge of data protection law, regardless the one who will be entrusted with the task is an employee or an outside consultant, lawyer or expert.

In addition, it is crucial to highlight whoever is selected to be in charge of the organisation's data protection office and whatever the person's academical background is, the nomination of a Data Protection Officer is associated to considerable alterations to the undertaking, namely from a structural nature.

Last but not least, *Softinsa* has not appointed its own Data Protection Officer yet but intends to do so such that the decision is still under discussion.

3.7. Technical and Organisational Measures

The implementation of Technical and Organisational Measures, commonly referred by the acronym TOMs, are one of the most important requirements of GDPR from the companies' perspective. TOMs are fundamentally mechanisms of defence against potential infractions of the GDPR that may result in data theft and loss, that corporations adopt in order to ensure compliance and also to attenuate the risk of exposure to data breach. TOMs will work, under the eyes of the data protection authorities, as a proof of the follow-up of procedures aimed at enhancing data protection and subject's security. In the alignment of the hiring of a Data Protection Officer, the implementation of these security and compliance-oriented measures might reflect a tremendous financial effort from *Softinsa* and the other undertakings, mainly due to the timeframe of each measure.

Before we go further on the Technical and Organisational Measures that the *IBM Group* has made available for its subsidiaries (*IBM Portugal* provides by its turn a set of those for *Softinsa*), there are two fundamental procedures that organisations will undertake on May 25th onwards. Apart from that, the introduction of the *Data Processing Agreement (DPA)*, that will alter *Softinsa*'s interaction with Clients, will also be explained.

Firstly, due to the heavy obligations for companies that GDPR's enforcement will introduce, undertakings are expected to assess the risk of data breach associated to their business operations. Impact Assessments[XIV] are tools, namely specific softwares, designed to aid organisations in studying and evaluating the potential risks of data breach associated to the processing activity the company performs. It must be enhanced that this impact measurement is performed internally.

Secondly, this new legal framework will lead to the adoption of Codes of Conduct[xv] that provide useful compliance-oriented approaches tailored to a specific industry or processing activity.

Bearing in mind that the new data protection law will pose duties for Controllers and Processors, as explained in section 3.2. of the Work Project, the roles and responsibilities of each party, concerning compliance, need to be as clear as possible. In order to distinguish the respective functions, a contract named *Data Processing Agreement* (or *Data Processing Addendum - DPA)* must be entered into between the Controller (Client) and the Processor (*Softinsa*). Although, there is a general template available for the DPA the addendum may be tailored for each corporation accordingly.

The DPA is a document that will impact on the interaction between *Softinsa* and its Clients. In order to ensure an accurate understanding of duties and responsibilities towards the legislation, as the GDPR gets into force, *Softinsa*, acting as a Processor, will be supposed to explain and clarify the terms and conditions set out in the DPA to Clients, jointly with an appendix that contains the proposed Technical and Organisational Measures. Once again, the duties of Controllers and Processors cited in sections 3.1. and 3.2. of the dissertation are invoked. It is a duty of *Softinsa* to inform the Client about the potential risks of data violation associated to a business activity and to play the role of advisor in indicating suitable TOMs to address and mitigate those risks. However, the ultimate decision on this matter is made by the Controller. Otherwise, *Softinsa* would be acting as a Controller and the responsibility in case of failure at data protection or even data breach would fall on itself.

Furthermore, in case there is no processing of personal data throughout a specific project with a specific Client, *Softinsa* is required to sign out a "green letter" with its Client, which exactly states the project will not imply any processing of personal data. Consequently, in this

occasion and only in this, *Softinsa* will be exempt of its duties as a Processor, under the GDPR guidelines.

TOMs designed by the *IBM Group*, addressed to *Softinsa* and to its other branches, are organised in 3 main groups: ***1 – Security Planning, 2 – Access Management, 3 – System & Network Security***. Within each group there is a set of diverse categories, as shown in Exhibit 1.

4. CONCLUSIONS & RECOMMENDATIONS

MAIN FINDINGS

The focus of this Work Project was to perform a critical analysis of the implications of the GDPR for *Softinsa*, what addresses the main objective of the Internship. Thus, we may conclude that the goals proposed for the Internship were accomplished.

According to a study[XVI] conducted by *KPMG Portugal* between November 2016 and January 2017, that encompassed over than 100 Portuguese organisations from a wide range of Sectors (Health, Finance, Retail, Services, Insurance, and Public), 65% of the participating undertakings detained a medium or high level of GDPR awareness. However, nearly 85% admitted not to have implemented any Technical and Organisational Measures so far and only approximately 15% of respondents have already nominated a Data Protection Officer. These findings are indicators that *Softinsa*, and the overall *IBM Group*, might be a step ahead as regard to the standard level of readiness of Portuguese companies concerning the GDPR enforcement.

Bearing in mind the exemplary level of readiness for GDPR enforcement and the timely implementation of Technical and Organisational Measures aimed at ensuring compliance concerning the *IBM Group* and its subsidiaries, there are no strategic recommendations for *Softinsa* on this matter.

MAIN RECOMMENDATIONS

Throughout this Work Project it was concluded that the enforcement of GDPR will translate itself on alterations within the company from a structural, behavioural and financial perspective. The usage of TOMs intends to address the first two implications. On the other hand, it leads to high implementation costs.

Thus, an opportunity arises to propose a cost monitoring process to *Softinsa*. It would serve to figure out the total costs of the overall compliance process to *Softinsa* 1 year after the enforcement of GDPR. This cost analysis will be mainly aimed at avoiding a waste of resources (time and money fundamentally), *from Softinsa*, by implementing TOMs as efficient as possible.

5. APPENDIX

Group Number	Category Name	TOM Description
1	Reviews, Assessments & Audits	Follow-up action plans resulting from security audits, tests and assessments
		Regularly assess project risks related to processing of personal data
	Risk Management & Incident Management	Document and management project and data processing risks, according to the risk management process
		Implement an effective emergency plan, ensuring adequate involvement of *Softinsa*'s Legal Department
	Project Management & People Management	Ensure personal data is only processed as agreed in the *DPA*
		Ensure availability of appropriate Data Security and Privacy (DS&P)
	Information Classification Scheme, Inventory & Data Map	Create and maintain an inventory of Client personal data and security related items
	Training	Define password handling rules in *Softinsa* corporate instructions and conduct annual training to foster employee awareness
2	Physical Access (access to buildings, Workplace Security, Environmental Security	Protect and control access to the systems containing Clients' personal data and to secured areas
	User Access Management (request, approve, grant, modify, revoke, revalidate)	Manage user access to the project technical environment
		Manage privileged accesses and shared users ID

	Logging and Monitoring of Access	Monitor and log read access to Client Personal Data
		Monitor and log privileged and shared users ID
	Data Backup, Disaster Recovery and Secure Deletion	Implement disaster recovery and backup capabilities to recover Clients personal data
3	Network and Firewalls, System Logging & Monitoring and Separation of Environments	Separate development & test environments (including the use of personal data) from the production environment
		Log and monitor system activities, according to the contract, plus the *DPA* and its respective exhibit
	Controls and Validation	Establish and adhere to the system and the application change process
		Implement testing and validation processes to ensure only authorised changes are promoted to production
	Data Protection Techniques	Employ the use of **encryption**, **pseudonymisation** or **anonymisation** of Client personal data in data processing activities, wherever it is applicable
	Physical Equipment and Media Handling	Encrypt portable storage media
		Securely destroy sensitive information and licensed software prior to reuse or disposal of equipment
	Development and Design	Follow privacy by design principles for new system

Exhibit 1 – *IBM Group* and its subsidiaries' Technical and Organisational Measures

6. REFERENCES

[I] Softinsa. 2017. "About Softinsa". Accessed February 15th 2018. http://www.softinsa.pt/section/softinsa

[II] European Union. 2018. "Regulations, Directives and other acts". Accessed February 12th 2018. https://europa.eu/european-union/eu-law/legal-acts_en

[III] European Union. 2016. "Regulation (EU) of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", **Article 4**.

[IV] European Union. 2016. "Regulation (EU) of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", (p. 1-31)

[V] European Union. (2016). "Regulation (EU) of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), **Recital 74**, (p. 14)

[VI] European Union. (2016). "Regulation (EU) of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", **Articles 24, 26 and 33**, (p. 47, 48 and 52)

[VII] TaylorWessing. 2016. "Obligations on data processors under the GDPR". Accessed March 3rd 2018. https://www.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html

[VIII] European Union. (2016). "Regulation (EU) of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", **Chapter 3, Sections 1-4, Articles 12-21** (p. 39-46)

[IX] Gabel, Dr. Detlev, and Hickman, Tim. 2017. "Chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation". Accessed March 10th 2018. https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation

[X] Allnutt, Hanns. 2018. "UK set to extend criminal offences to directors and officers for breaches of GDPR". Accessed February 27th 2018. http://views.dacbeachcroft.com/post/102eqw5/uk-set-to-extend-criminal-offences-to-directors-and-officers-for-breaches-of-gdpr

[XI] Crendo Insurance Brokers. 2016. "GDPR Emphasises Accountability of Directors and Officers". Accessed March 2nd 2018. http://www.crendoninsurance.co.uk/wp-content/uploads/2013/10/Cyber-Risks-and-Liabilities-Newsletter-March-April-2016.pdf

[XII] Crendo Insurance Brokers. 2016. "GDPR Emphasises Accountability of Directors and Officers". Accessed March 4th 2018. http://www.crendoninsurance.co.uk/wp-content/uploads/2013/10/Cyber-Risks-and-Liabilities-Newsletter-March-April-2016.pdf

[XIII] Signaturit. 2016. "GDPR: What is the role of the Data Protection Officer and when will it be mandatory to incorporate one into companies?". Accessed April 3rd 2018. https://blog.signaturit.com/en/what-is-the-role-of-a-data-protection-officer-and-when-will-it-be-mandatory-to-incorporate-one-into-companies

[XIV] Gabel, Dr. Detlev, and Hickman, Tim. 2017. "Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation". Accessed March 30th 2018. https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data

[XV] Gabel, Dr. Detlev, and Hickman, Tim. 2017. "Chapter 12: Impact Assessments, DPOs and Codes of Conduct – Unlocking the EU General Data Protection Regulation". Accessed March 30th 2018. https://www.whitecase.com/publications/article/chapter-12-impact-assessments-dpos-and-codes-conduct-unlocking-eu-general-data

[XVI] KPMG Portugal. 2017. "O Impacto do Regulamento Geral da Protecção de Dados em Portugal". Accessed April 4th 2018. https://assets.kpmg.com/content/dam/kpmg/pt/pdf/pt-2017-rgpd.pdf

7. FURTHER RESEARCH

At the final of each year, from May 25th 2019 onwards, what this Work Project recommends to *Softinsa* is to display the implemented TOMs, on an Implementation Cost vs Impact on compliance matrix (the template is on Exhibit 2).

A TOM's Implementation Cost includes the financial cost, the timeframe for its implementation, how long it takes to be implemented and eventual maintenance costs (e.g encrypting a disk requires a license and periodic reviews to verify if the information remains unreadable to unauthorized people). Moreover, the Impact of a TOM is associated to its capacity of aiding *Softinsa* to comply with the GDPR framework and to avoid potential data breaches and data subjects' security violation.

The challenge concerning this procedure would be to identify the measures presenting a low implementation cost and a high impact, the *Quick wins*, and to attempt to replicate them; then, those that present a balance between a high implementation cost and high impact on compliance, constituting an *Investment*, should be kept and improved; the costly and low impact on compliance with GDPR initiatives should be eliminated, since they integrate the *Money expended* zone of the diagram. Finally, the company should quit from Technical and Organisational Measures with a low cost and low impact on compliance, since they enter directly into the *Time expended* quadrant measures.

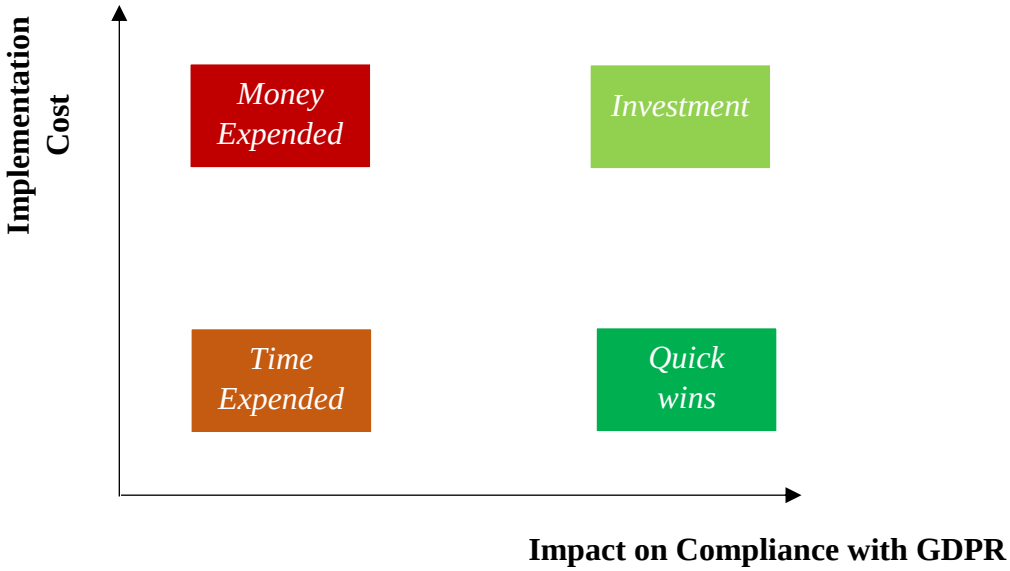

Exhibit 2 – Impact vs Implementation Cost Matrix